UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/507,478	02/17/2000	Henrique Malvar	MS1-338US	7435

22801 7590 02/09/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
MEISLAHN, DOUGLAS J	

ART UNIT	PAPER NUMBER
2137	6

DATE MAILED: 02/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/507,478	Applicant(s) MALVAR ET AL.	
	Examiner Douglas J. Meislahn	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-57 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-57 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 17 February 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: in line 20 of page 5, "a" needs to be inserted before "thief".

Appropriate correction is required.

Claim Objections

2. Claim 2 is objected to because of the following informalities: "comprises" should not be singular – change it to "comprise". Appropriate correction is required.

3. Claims 19, 20, and 48 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 48 changes the statutory class and as such does not limit the method. Claims 19 and 20 claim, respectively, a media player and operating system, neither of which limits the content scrambler of their parent claim. Rewrite the claims in independent form.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

> only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 25 and 27 are rejected under 35 U.S.C. 102(b) as clearly anticipated by Nicolai et al. (4188580). See Nicolai et al.'s abstract.

6. Claim 52 is rejected under 35 U.S.C. 102(e) as being anticipated by Shepard (6598164).

In the second box down on the right of figure 4, a provider (which reads on applicant's server) scrambles and then compresses a selection, which is content. This anticipates the first two clauses of claim 52. In the box below, the encrypted, compressed data is sent to a customer, who reads on applicant's client. Thus is the third clause anticipated. In lines 18-41 of column 2, Shepard describes decompressing data and returning the decompressed data to a storage device. The decompression clearly reads on applicant's fourth clause. Data transfer is a type of processing and thus reads on the fifth clause. The content is then descrambled and output, thereby anticipating the last two clauses of claim 52.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 2, 5, 8, 10, and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over applicant's admitted prior art in view of Hogan (6047069).

Figure 2 of applicant's disclosure, which is labeled as prior art, presents one of more output devices (element 44), a content player (element 52), and a processor (element 64). The operation of these elements requires a processor, a memory, and an operating system. As such, the limitations of the first five clauses of claim one are met. This prior art diagram does not say that data is scrambled before being processed, or that it is decrypted after the processing. In his abstract, figure 7, and lines 7-30 of column 5, Hogan teaches processing data while it is encrypted, thereby preventing access to confidential data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to keep data encrypted during its processing, as taught by Hogan, to protect data from illicit viewing.

Claim 2 is obvious because applicant's background section teaches filter graphs as being used in processing. Claim 5 is rendered obvious by lines 18-20 of column 2, which teach XORing to effect scrambling. The limitations of claim 8 are shown by the same three lines, which teach that the added data be random. Claim 10 is obvious because the random data block can be viewed as a key. Claim 14 is obvious because of the structure of the admitted prior art.

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over applicant's admitted prior art and Hogan as applied to claim 1 above, and further in view of Schneier (*Applied Cryptography*).

Hogan, as applied to applicant's admitted prior art, teaches processing data while the data is encrypted in order to protect the data. Neither reference mentions receiving the data, in encrypted, compressed form, from an outside source. On page 226,

Schneier gives reasons to both encrypt and compress data: the amount of data is reduced, security is increased, etc. The section also implicitly teaches transmission. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to receive encrypted, compressed data from an outside source, as taught by Schneier, and to decrypt and decompress that data at the media player in applicant's admitted prior art.

10. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over applicant's admitted prior art and Hogan as applied to claim 1 above, and further in view of Nyström et al. (6526091).

Hogan, as applied to applicant's admitted prior art, teaches processing data while the data is encrypted in order to protect the data. Neither reference mentions that the encryption adds a noise signal. In lines 15-18 of column 5, Nyström et al. show the addition of pseudo-random noise as a means to scramble data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for the encryption in Hogan to add a noise signal, as taught by Nyström et al.

11. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over applicant's admitted prior art and Hogan as applied to claim 1 above, and further in view of Bae (5991416).

Hogan, as applied to applicant's admitted prior art, teaches processing data while the data is encrypted in order to protect the data. Neither reference mentions time-domain or frequency-domain scrambling as the preferred method of scrambling. In lines 19-24 of column 1, Bae teaches four scrambling techniques, two of which are time-

domain and frequency-domain, used to obscure voice data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use time-domain or frequency-domain scrambling in applicant's admitted prior art when the data is voice data, which is common in today's communications.

12. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over applicant's admitted prior art and Hogan as applied to claim 1 above, and further in view of Marzahn (6526145).

Hogan, as applied to applicant's admitted prior art, teaches processing data while the data is encrypted in order to protect the data. According to the combination, encryption is performed by the content player. Neither reference mentions that a descrambler is resident on a driver for the output device. In lines 16-22 of column 1, Marzahn teaches driver decryption as a way to implement a transparent encryption system. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement decryption in the output device driver as taught by Marzahn in order to transparently protect the data.

13. Claims 4, 9, and 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant's admitted prior art and Hogan as applied to claim 1 above, and further in view of Nicolai et al. (4188580).

Hogan, as applied to applicant's admitted prior art, teaches processing data while the data is encrypted in order to protect the data. Neither reference mentions uses a sync tone and random signal. In their abstract, Nicolai et al. describe embedding a first signal (tracking data) representing a first key into data, basing a

second signal (pseudo-random signal) on the first signal and on a second key (pseudo-random number generator's inherent seed), and embedding the second signal in the data also. While Nicolai et al. explicitly only states that the second key is used to generate the pseudo-random signal, the tracking data is clearly used in the pseudo-random signal's regulation and hence creation. Nicolai et al.'s system prevents loss of synchronization. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ Nicolai et al.'s scrambling system in the combination of applicant's admitted prior art and Hogan.

With respect to claim 12, the channel on which the seed is sent to the two entities (or transmitted from one to the other) is at least temporally separate from the channel used for the scrambled content. Claim 13 is rendered obvious by Hogan who, in lines 32-34 of column 5, teaches securely transmitting a random number generator's seed.

14. Claims 15-17, 19-24, 26, 29, 32-35, and 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nicolai et al. (4188580) in view of the *Microsoft Press Computer Dictionary*, 3rd ed.

Figure 9B and elements 11 and 13 of figure 1 anticipate a tone generator and modulator that creates a periodic set of tone patterns. As described in lines 22-30 of column 4, the tones, described by Nicolai et al. as a tracking or masking signal, provide a masking function and thus anticipate a first key. As shown in figure 1, the outputs of elements 11 and 13 find their way to the pseudo-random number generator (element 10). The pseudo-random number generator anticipates applicant's random number generator. (Applicant uses the phrase "random number generator", which

encompasses both pseudo-random number generators and truly random RNGs: the examiner believes the latter would be unworkable in applicant's invention.) The second key is sent by the code select (element 76). As described in the abstract, the first key (as the tracking signal) and the pseudo-random generator output are added to the signal, thereby anticipating the third clause of claim 15. See also elements 33 and 36 in figure 1. Nicolai et al. do not say that the first key is embodied in the tracking signal as amplitude modulations. The definition of amplitude modulation in the computer dictionary defines it as encoding data in a constant frequency transmission by varying amplitude. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include the first key of Nicolai et al. in the tracking signal by modulating the amplitude of the tracking signal, as is well known in the art of computer communications.

The limitations of claim 16 are encompassed by the above discussion. Claim 17 is obvious because bit-value communications are anticipated by computer communications. Claims 19 and 20 include the same limitations as claim 15. Claims 21-24 pertain to descrambling and are rendered obvious by the elements cited above.

With respect to claims 26 and 29, Nicolai et al. teach a system in which tow keys are used to form a scrambling signal. One of the keys is included with the encrypted information. They do not say that the scrambling and descrambling are implemented within and operating system. The computer dictionary teaches operating systems as controlling resources. Implementing the functions in software, as opposed to hardware, would make the process accessible to computers that lack the hardware. Therefore it

would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the system of Nicolai et al. in software such as an operating system.

Claims 32-35 are rendered obvious for the same reasons as claims 15-17 and 21. Claims 55-57 are computer readable media for the limitations of claims 15 and 21.

15. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nicolai et al. and the *Microsoft Press Computer Dictionary*, 3rd ed. as applied to claim 15 above, and further in view of Schneier (*Applied Cryptography*).

Nicolai et al. and the dictionary present a system in which two keys are used to form a scrambling signal. One of the keys is included with the encrypted information. The second key is formed by code select. They do not say that the second key is encrypted for secure transportation to a descrambler. On page 176, Schneier teaches key-encryption keys, which encrypt other keys for distribution. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the second key in Nicolai et al. using a key-encrypting key, as taught by Schneier. Nicolai et al. need a second key to seed the code select.

16. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nicolai et al. in view of Hogan.

Nicolai et al. teach a system in which tow keys are used to form a scrambling signal. One of the keys is included with the encrypted information. They do not say that the scrambling and descrambling both occur at the recipient. Hogan presents a system that scrambles content before it is processed and then descrambles the content after

processing, thereby protecting the content during processing. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the scrambling and descrambling of Nicolai et al. at a receiver, thereby protecting the data during processing as taught by Hogan.

17. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nicolai et al. in view of Marzahn (6526145).

Nicolai et al. teach a system in which tow keys are used to form a scrambling signal. One of the keys is included with the encrypted information. They do not say that a descrambler is resident on a driver for the output device. In lines 16-22 of column 1, Marzahn teaches driver decryption as a way to implement a transparent encryption system. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement decryption in the output device driver as taught by Marzahn in order to transparently protect the data.

18. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nicolai et al. in view of Schneier (*Applied Cryptography*).

Nicolai et al. present a system in which two keys are used to form a scrambling signal. One of the keys is included with the encrypted information. The second key is formed by code select. They do not say that the second key is encrypted for secure transportation to a descrambler. On page 176, Schneier teaches key-encryption keys, which encrypt other keys for distribution. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the second key in Nicolai et al. using a key-encrypting key, as taught by Schneier. Nicolai

et al. need a second key to seed the code select. Encrypted communications form a cryptographically secure path.

19. Claims 36, 39-41, 43-44, and 48-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nicolai et al. and Hogan as applied to claim 28 above, and further in view of Schneier.

Nicolai et al. and Hogan teach encrypting data at a client, processing the encrypted data, and then decrypting and playing the data. They do not say that the data is encrypted and compressed for transmission from the server to the client. On page 226, Schneier gives reasons to both encrypt and compress data: the amount of data is reduced, security is increased, etc. The section also implicitly teaches transmission. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to receive encrypted, compressed data from an outside source, as taught by Schneier, and to decrypt and decompress that data at the media player in Nicolai et al. and Hogan.

20. Claims 37, 38, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nicolai et al., Hogan, and Schneier as applied to claims 36 and 39 above, and further in view of applicant's admitted prior art and Marzahn.

Nicolai et al., Schneier, and Hogan teach encrypting data at a client, processing the encrypted data, and then decrypting and playing the data. They do not say that the scrambler is implemented in the scrambler or that the descrambler is in the driver. Applicant's admitted prior art puts the scrambler in the media player. Marzahn teaches driver decryption. Therefore it would have been obvious to a person of ordinary skill in

the art at the time the invention was made for the scrambler to be embodied in the media player and for the driver to contain the descrambler. Operating systems controls the operations of a computer. Claim 47 is rendered obvious because applicant's admitted prior art teaches filter graphs.

21. Claim 42 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nicolai et al., Hogan, and Schneier as applied to claim 39 above, and further in view of Bae.

Nicolai et al., Schneier, and Hogan teach encrypting data at a client, processing the encrypted data, and then decrypting and playing the data. They do not say that time-domain or frequency-domain scrambling is the preferred method of scrambling. In lines 19-24 of column 1, Bae teaches four scrambling techniques, two of which are time-domain and frequency-domain, used to obscure voice data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use time-domain or frequency-domain scrambling in Nicolai et al.

22. Claims 45 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nicolai et al., Hogan, and Schneier as applied to claim 39 above, and further in view of the *Microsoft Press Computer Dictionary*, 3rd ed.

Nicolai et al., Schneier, and Hogan teach encrypting data at a client, processing the encrypted data, and then decrypting and playing the data. They do not say that the first key is embodied in the tracking signal as amplitude modulations. The definition of amplitude modulation in the computer dictionary defines it as encoding data in a constant frequency transmission by varying amplitude. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to

include the first key of Nicolai et al. in the tracking signal by modulating the amplitude of the tracking signal, as is well known in the art of computer communications.

23. Claims 53 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shepard in view of Nicolai et al. and the *Microsoft Press Computer Dictionary*, 3rd ed.

Shepard presents a system that keeps digital data in encrypted form, only decrypting while changing the data to analog form. He does not specify how the encryption is implemented. Nicolai et al. and the computer dictionary (as described above) present a system that scrambles data by adding periodic tones modulated by a first key and a pseudo-random signal based on both the first key and a second key. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the scrambling system of Nicolai et al. with Shepard so that the encryption would be applicable to both analog and digital signals.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Douglas J. Meislahn
Examiner
Art Unit 2137

DJM